DETAILED ACTION

Claims 1-45 are pending.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Amendment and Arguments

Applicant's amendments were fully considered. Applicant's arguments directed at the amended claims were also fully considered, but are not persuasive. The limitation that applicant argues makes the claims allowable over the prior art of record is already disclosed by prior art of record. See for example, applicant's own admitted prior art discussed in paragraph 6 of the specification as well as Lachman as discussed below.

Claim Objections

Claims 23-25, 28-30, and 35 are objected to because of the following informalities: In these claims, all instances that "the terminal device" and "the server" should instead be "the at least one terminal device" and "the at least one server" respectively so as to be consistent with what is recited in lines 3-4 of claim 23. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 10-22, 33-34, and 39-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 10-22 and 33-34 either directly or via dependency refer to "computer readable medium". The term “computer readable medium” is not defined in the specification, thus the metes and bounds of the claim cannot be determined. It is unclear if the term is meant to also encompass signals or not since the term is not defined. If applicant believes the term is defined in the specification, it is requested that applicant specifically and clearly point out where the term is defined and the metes and bounds are set.

Claim 39 as recited appears to either have missing words form the clause or be grammatically incorrect. The meaning of the limitation cannot be determined.

Claims not specifically addressed are rejected due to dependency.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 10-22 and 33-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 10 is directed towards a system comprising at least one computer readable medium including various modules configured to perform various tasks.

Because computer readable medium is not defined in the specification, it is submitted that the term could broadly, but reasonably be interpreted to refer to signals. As such, Claim 10 appears to be directed to a system comprising a signal per se including various software modules encoded within the signal. Signals per se does not fall within any of the four statutory categories of invention, thus claim 10 and its dependent claims (claims 11-15 and 33) are not statutory.

Claims 16-22 and 34 are also not statutory for similar reasons since these claims also are directed towards a computer readable medium, which is a term not defined in the specification and could be broadly, but reasonably be interpreted to refer to a signal.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 10, 16, 23, 3, 30-35, 13, 19, 27, 7, 14, 20, 28, 9, 15, 22, 29, 11, 24, 18, 25, 36, and 42-43 are rejected under 35 U.S.C. 102(b) as being anticipated by Lachman III et al (US 2002/0166063).

Claims 1, 10, 16, and 23:

As per claim 23, Lachman discloses:

1. At least one terminal device (Fig 1, host server 102).

2. At least one server (Fig 1, system 106 and server 108) coupled to a computer network and to the terminal device (Fig 1), wherein the server is configured to monitor packets directed to the terminal device (paragraph 70), the at least one server having one or more modules (Fig 2, i.e. software modules), including:
    a. A detection module configured to:
        i. Monitor one or more packets received from a source device to determine whether one or more of the received packets include one or more harmful computer code signatures (paragraph 98), and to further monitor the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the terminal device (paragraphs 19, 107, 111, and 114-116).
        ii. Detect an attack directed at the terminal device if one or more of the monitored packets include one or more of the harmful computer code signatures (paragraph 17), and to further detect the attack if one or more of the monitored packets include the identifying information that has the history of being included in the packets associated with the previous attacks directed at the terminal device (paragraphs 19, 100, 107, 109, and 111).
    b. A log creating module configured to create an attack profile based on information associated with the detected attack, wherein the attack profile

provides identifying information included in one or more of the monitored packets that include the harmful computer code signatures (paragraphs 73, 84, and 89), and wherein the attack profile further provides the identifying information that has the history of being included in packets associated with the previous attacks directed at the at least one terminal device (paragraphs 73, 84, 91-92, 99, 107, and 109).

c. A scanning module configured to determine a severity of the directed attack directed at the terminal device (paragraphs 85, 101-102, 105, 130, 153, and 185).

d. A blocking module configured to:

    i. Block one or more of the monitored packets from being transmitted to the at least one terminal device, wherein the blocked packets include the identifying information provided in the attack profile (paragraphs 111 and 116).

    ii. Block one ore more subsequently received packets from being transmitted to the at least one terminal device if the severity of the detected attack exceeds a predetermined threshold, wherein the subsequently blocked packets include packets originating from the source device and packets directed to the terminal device (paragraphs 101, 111-112, 116, 120, and 150).

Claims 1, 10, and 16 contain similar limitations as claim 23 and are rejected for similar reasons cited above.

Claim 3:

Lachman further discloses wherein the identifying information provided in the attack profile identifies at least one of a source Internet Protocol address, a source port number, a destination Internet Protocol address, or a destination port number associated with the detected attack (paragraph 107).

Claim 30:

Lachman further discloses wherein the server is further configured to issue an alert to inform an administrator of the network of detected attack directed at the terminal device (paragraph 185).

Claim 31:

Lachman further discloses wherein the subsequently blocked packets include information identifying one or more of the source Internet Protocol address, the source port number, the destination Internet Protocol address, or the destination port number (paragraphs 107 and 111).

Claims 32, 33, 34, and 35:

Lachman further discloses wherein the attack profile further provides identifying information included in one or more packets associated with one or more of suspected or confirmed attacks directed at the target system (paragraphs 20 and 73-74).

Claims 13, 19, and 27:

Lachman further discloses wherein the scanning modules is further configured to determine the severity of the detected attack based on at least one of frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets (paragraphs 101-102 and 130-131).

Claims 7, 14, 20, and 28:

Lachman further discloses wherein blocking the packets from being transmitted to the target system includes instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel connecting the source system to the target system (paragraph 120).

Claims 9, 15, 22, and 29:

Lachman further discloses wherein blocking the subsequently received packets from being transmitted to the target system expires after at least one of a predetermined amount of time, a predetermined period of inactivity, or an occurrence of a triggering event (paragraphs 113 and 125).

Claims 11 and 24:

Lachman further discloses wherein the log creating module is further configured to store, in the database, identifying information included in one or more packets associated with suspected or confirmed attacks directed at the at least one terminal device (paragraph 84).

Claim 18:

Lachman further discloses wherein the received packets are stored in a storage buffer and monitored upon release from the storage buffer (Fig 2). The packets goes through the router/firewall 204 whose memory can be considered a storage buffer. After exiting the router/firewall 204, the packets are scanned in one of the workstations.

Claim 25:

Lachman further discloses a database coupled to the at least one server (Fig 2).

Claim 36:

Lachman further discloses wherein disabling the communication channel causes packets that are suspected or confirmed of attacking the target system to be contained within the target system (paragraphs 115-116).

Claim 42:

Lachman further discloses wherein the attack profile further provides information identifying a time of day and a frequency that the monitored packets were received (paragraph129 and Fig 11).

Claim 43:

Lachman further discloses wherein the subsequently blocked packets further include the identifying information provided in the attack profile (paragraphs 90-92 and 107).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 12, 26, 4-6, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lachman III et al (US 2002/0166063) in view of Shetty (US 6,772,345).

Claims 2, 12, and 26:

The limitation of wherein the identifying information provided in the attack profile identifies a type of communication associated with the detected attack is disclosed by Shetty (col 3, lines 12-40).

It would have been obvious to one skilled in the art to modify Lachman's invention using Shetty's to include the above limitation. One skilled would have been motivated to incorporate Shetty's teachings because Shetty's teachings would allow malware scanning of transmitted data to occur at the protocol level, which would enable Lachman's invention to thereby block the spread of malware that may not be blocked by operating system level scanning (Shetty: col 1, lines 57-62).

Claim 4:

The combination of Lachman and Shetty further discloses wherein the type of communication associated with the detected attack includes at least one of File Transfer Protocol, Simple Mail Transfer Protocol, Telnet, Domain Name System, Windows

Internet Name System, HyperText Transfer Protocol, Traceroute, instant messaging, or chat (Shetty: col 3, lines 12-40).

Claim 5:

The combination of Lachman and Shetty further discloses wherein the received packets are monitored using Transmission Control Protocol/Internet Protocol at an application layer to characterize the type of communication associated with the packets originating from the source system (Shetty: col 3, lines 58-60).

Claim 6:

Lachman further discloses determining the severity of the detected attack based on at least one of frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets (paragraphs 101-102 and 130-131).

Claim 17:

The limitation of wherein the received packets are monitored transparently in real time is disclosed by Shetty (col 1, lines 57-60 and col 4, lines 15-17).

It would have been obvious to one skilled in the art to modify Lachman's invention according to Shetty's teachings as recited in claim 17. One skilled would have been motivated to incorporate Shetty's teachings in Lachman's for the same reasons discussed in claim 2.

Claims 8 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lachman III et al (US 2002/0166063) in view of Alampalayam et al ("An Adaptive Security Model for Mobile Agents in Wireless Netowrks"), herein referred to as Alam.

Claims 8 and 21:

The limitation of notifying the source system that the attack has been detected and that a block was placed on packets received form the source system is disclosed by Alam (p1519, Step 3: Protection Framework" section).

It would have been obvious to one skilled in the art to modify Lachman's invention using Alam's teachings according to the limitations recited in claims 8 and 21. One skilled would have been motivated to do so because sometimes a source system were themselves attacked and the user may not know that their system has been used for causing attacks on other systems. This is usually due to the source system having been infected with a virus which uses the source system for attacks. Alerting the source system would allow the users of the source system to take appropriate measures to prevent further unauthorized use of their system for unauthorized attacks.

Claims 38 and 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lachman III et al (US 2002/0166063) in view of Smithson et al (US 6,886,099).

Claim 38:

The limitation of correlating a pattern for the detected attack to the severity of the detected attack to determine the amount of time and the period of inactivity after which blocking the subsequently received packets from being transmitted to the target system expires is disclosed by Smithson (col 6, lines 34-58 and col 8, lines 44-58).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Lachman's invention according to the limitations further recited in claim 38. One skilled would have been motivated to do so because it would allow adaptive scaling of response in accordance with the severity of an attack, which would provide for a more flexible attack prevention system.

Claim 44:

The limitation of permanently blocking subsequently received packets originating from the source system from being transmitted to the target system if the severity of the detected attack indicates that the source system is a habitual attacker of the target system is made obvious over Smithson's teachings (col 6, lines 34-58 and col 8, lines 44-58).

It would have been obvious to modify Lachman's teachings according to the limitations further recited in claim 44 in light of Smithson's teachings. One skilled would have been motivated to do so because it is common sense to permanently block habitual attackers.

Claim 45:

Lachman and Smithson further teaches the limitation of wherein a user can manually reset the permanent block on the subsequently received packets originating from the source system to allow a flow of packets originating form the source system to the target system (Smithson: col 6, lines 34-58 and col 8, lines 44-58).

Allowable Subject Matter

Claim 37 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Examiner, Art Unit 2435